

AO 106 (REV 4/10) Affidavit for Search
Warrant

AUSA Karlin Klamann (312) 353-5361

FILED
5/24/2021
CCUNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISIONTHOMAS G. BRUTON
CLERK, U.S. DISTRICT COURT**UNDER SEAL**

In the Matter of the Search of:

Case Number: 21 CR 316

the three Trak4 vehicle tracking devices and
associated equipment, further described in
Attachment A**APPLICATION AND AFFIDAVIT FOR A SEARCH WARRANT**

I, Holly Groff, a Special Agent of the Federal Bureau of Investigation, request a search warrant and state under penalty of perjury that I have reason to believe that on the following property or premises:

See Attachment A

located in the Northern District of Illinois, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is evidence and instrumentality.

The search is related to a violation of:

*Code Section**Offense Description*

Title 18, United States Code, Sections 875(c), 2261A

Interstate threats; cyberstalking

The application is based on these facts:

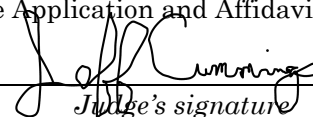
See Attached Affidavit,

Continued on the attached sheet.

s/Holly Groff - by consent/JC

*Applicant's Signature*HOLLY GROFF, Special AgentFederal Bureau of Investigation*Printed name and title*

Pursuant to Fed. R. Crim. P. 4.1, this Application is presented by reliable electronic means. The above-named agent provided a sworn statement attesting to the truth of the statements in the Application and Affidavit by telephone.

Date: May 24, 2021
*Judge's signature*City and State: Chicago, IllinoisJEFFREY CUMMINGS, U.S. Magistrate Judge*Printed name and title*

UNITED STATES DISTRICT COURT)
)
NORTHERN DISTRICT OF ILLINOIS)

AFFIDAVIT

I, Holly Groff, being duly sworn, state as follows:

1. I am a Special Agent with the Federal Bureau of Investigation (FBI). I have been so employed since approximately June 2014. My current responsibilities include the investigation of criminal violations relating to sex trafficking, with an emphasis on sex trafficking of minors, in violation of Title 18, Unites States Code, Sections 1591, child exploitation and child pornography, in violation of Title 18, Unites States Code, Sections 2252, 2252A. I have received training in the area of sex trafficking, child pornography, and child exploitation.

2. This affidavit is made in support of an application for a warrant to search four Trak4 vehicle tracking devices and associated equipment (the “**Subject Devices**”), for evidence and instrumentalities described further in Attachment B, concerning interstate threats and cyberstalking offenses, in violation of Title 18, United States Code, Sections 875(c) and 2261A (“the **Subject Offenses**”).

3. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts

that I believe are sufficient to establish probable cause to believe that evidence and instrumentalities of violations of Title 18, United States Code, Sections 875(c) and 2261A, are located within the **Subject Devices**.

I. FACTS SUPPORTING PROBABLE CAUSE TO SEARCH THE SUBJECT COMPUTER

4. As explained below, on May 24, 2021, during the execution of a search warrant in this investigation, law enforcement recovered three Trak4 vehicle tracking devices and associated equipment, as described in Attachment A. As discussed in greater detail below, during the investigation, law enforcement spoke with a former employee of SCHWARTZ who informed law enforcement that s/he had a discussion with SCHWARTZ about SCHWARTZ installing a vehicle tracking device on his ex-girlfriend's car ("Individual A"). Based on this information and the discovery of vehicle tracking devices in SCHWARTZ's home, I believe there is probable cause to believe that the **Subject Devices** are evidence and instrumentalities of the **Subject Offenses**.

A. Warrant for the Subject Premises

5. On May 20, 2021, Magistrate Judge Jeffrey I. Cummings signed a warrant to search the residence located at 1511 Guthrie Drive in Inverness, Illinois ("**Subject Premises**"). On May 23, 2021, Magistrate Judge Jeffrey I. *See* 21 CR 316. Cummings signed an amended warrant to search the **Subject Premises**. The Affidavits supporting those warrants are referenced and incorporated herein.

B. The Subject Devices May Have Been Used to Track Individual A's Vehicle.

6. On or about May 20, 2021, this Affiant spoke with a former employee of SCHWARTZ ("Individual C," as referenced in the Affidavit support the search of the **Subject Premises**). Individual C told this Affiant that in or around December 2020, SCHWARTZ asked Individual C about installing a tracking device on Individual A's vehicle. Individual C stated that s/he refused to help SCHWARTZ install the devices. Individual C told this Affiant that s/he asked a friend to send Individual A a text message on or about December 31, 2020 warning Individual A that there may be a tracker on Individual A's vehicle.

7. During the investigation, law enforcement interviewed Individual A. Individual A told law enforcement that on or about December 31, 2020, Individual A received a text message from phone number XXX-XXX-0451, reading "Check under your car for a tracker from mr Schwartz...Did you get the red letter by your condo. An angel told me to let you know..."

C. The Subject Devices.

8. On or about May 24, 2021, law enforcement executed the warrant for the **Subject Premises**. During the search, law enforcement located three grey devices inside a safe located in a home office at the **Subject Premises**. One of the three gray devices had a sticker on it that read "Trak4," along with other information.

9. According to Trak4's website¹, the company sells a GPS tracker for "Tracking Assets, Equipment and Vehicles" for \$48.80. The color, size and shape of the device depicted on Trak4's website fits the description of the three gray **Subject Devices**. One of the gray devices also has what appears to be a magnet strip affixed to the back, as depicted in Attachment A. According to Trak4's website², the company sells an adhesive magnet kit for \$8.95 which can be used to "mount your Trak-4 GPS tracker to vehicles, trailers, tractors, and equipment..."

10. In addition to the three gray devices, the safe also contained a yellow metal rectangular device that has five antennae extending from one end. The device has an on/off switch on one side and perforated holes on the front.

II. SPECIFICS REGARDING SEARCHES OF ELECTRONIC STORAGE MEDIA

11. Based upon my training and experience, and the training and experience of specially trained personnel whom I have consulted, searches of evidence from electronic storage media commonly require agents to download or copy information from the electronic storage media and their components, or remove most or all electronic storage media items (*e.g.* computer hardware, computer software, computer-related documentation, and cellular telephones) to be processed later by a

¹ <https://shop.trak-4.com/> (last visited May 24, 2021).

² <https://shop.trak-4.com/collections/frontpage/products/adhesive-magnet-kit> (last visited May 24, 2021).

qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Electronic storage media can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.

b. Searching electronic storage media for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of an electronic storage media system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since electronic storage media evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

12. In order to fully retrieve data from a computer system, the analyst needs all storage media as well as the computer. The analyst needs all the system software

(operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard disk drives or on external media).

13. In addition, electronic storage media such as a computer, its storage devices, peripherals, and Internet connection interface may be instrumentalities of the crime(s) and are subject to seizure as such if they contain contraband or were used to carry out criminal activity.

III. PROCEDURES TO BE FOLLOWED IN SEARCHING ELECTRONIC STORAGE MEDIA

14. Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant will authorize the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol.

15. The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B;

d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

16. The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.

IV. CONCLUSION

17. Based on the above information, I respectfully submit that there is probable cause to believe that interstate threats and cyberstalking offenses, in


violation of Title 18, United States Code, Sections 875(c) and 2261A, have been committed, and that evidence and instrumentalities relating to this criminal conduct, as further described in Attachment B, will be found in the **Subject Devices**, as further described in Attachment A. I therefore respectfully request that this Court issue a search warrant for the **Subject Devices** more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B, pursuant to the protocol described in the addendum to Attachment B.

FURTHER AFFIANT SAYETH NOT.

s/Holly Groff - by consent/JC

Holly Groff
Special Agent
Federal Bureau of Investigation

Sworn to and affirmed by telephone 24th day of May, 2021



Honorable JEFFREY CUMMINGS
United States Magistrate Judge

ATTACHMENT A

DESCRIPTION OF ITEM TO BE SEARCHED

Three gray rectangular boxes each with six small screws affixed to the back of the devices. One gray device has a sticker affixed to the back and bears IMEI number 015058000389164, as depicted below. One gray device is partially deconstructed bearing IMEI number 015058000263369. One yellow rectangular metal device with five black antennae. The items are depicted in the photographs below:





ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

Evidence and instrumentalities concerning violation of Title 18, United States Code, Sections 875(c) and 2261A:

1. One gray Trak4 vehicle tracking device with no visible IMEI or serial number.
2. One partially deconstructed gray Trak4 vehicle tracking device bearing IMEI number 015058000263369.
3. One gray Trak4 vehicle tracking device with sticker bearing IMEI number 015058000389164.
4. One rectangular metal yellow device with five black antennae.
5. Any and all electronic data contained on the Subject Devices and associated equipment.

ADDENDUM TO ATTACHMENT B

Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant authorizes the removal of electronic storage media and copying of electronically stored information found in the premises described in Attachment A so that they may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol:

The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B; and
- d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.